UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/549,443	12/14/2006	Naoto Kuroda	9319Y-1318/NP	9507

27572 7590 10/21/2008
HARNESS, DICKEY & PIERCE, P.L.C.
P.O. BOX 828
BLOOMFIELD HILLS, MI 48303

EXAMINER	
CHAI, LONGBIT	

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
10/21/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/549,443	KURODA, NAOTO	
	Examiner	Art Unit	
	LONGBIT CHAI	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 September 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 September 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *9/16/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. Applicant's claim for benefit of foreign priority under 35 U.S.C. 119 (a) – (d) is acknowledged.

The application is filed on 12/14/2006 but is a 371 case of PCT/JP04/03533 application filed on 3/17/2004 and has a foreign priority application filed on 3/17/2003.

Claim Rejections - 35 USC § 101

35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 16 and 17 are rejected under 35 U.S.C. 101 because these claims are directed to "A network security enhancing program", which is merely an example of functional descriptive material, (i.e. software per se), and is nonstatutory under 35 USC 101. By not limiting the computer program product to being stored / embedded on a computer readable storage medium, there is a lack of the required functional and structural interrelationship between the software and the computer storage medium that permits the functionality of the software to be realized upon access by a processor. This ability is what underlies the ability to provide a practical application. Warmerdam, 33 F.3d at 1361, 31 USPQ2d at 1760. In re Sarkar, 588 F.2d 1330, 1333, 200 USPQ

132, 137 (CCPA 1978). See MPEP § 2106 (IV.B).1(a). Any other claims not addressed are rejected by virtue of their dependency.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

3. Claims 7 and 15 are rejected under 35 U.S.C. 112, first paragraph because **a single means claim**, i.e., where a means recitation does not appear in combination with another recited element of means, is subject to an undue breadth rejection under 35 U.S.C. 112, first paragraph. *In re Hyatt*, 708 F.2d 712, 714-715, 218 USPQ 195, 197 (Fed. Cir. 1983) (A single means claim which covered every conceivable means for achieving the stated purpose was held nonenabling for the scope of the claim because the specification disclosed at most only those means known to the inventor.). When claims depend on a recited property, a fact situation comparable to Hyatt is possible, where the claim covers every conceivable structure (means) for achieving the stated property (result) while the specification discloses at most only those known to the inventor. Any other claims not addressed are objected by virtue of their dependency should also be corrected.

Claim Objections

4. Claim 9 is objected to because of the following informalities: "is no connected" should be replaced with "is not connected". Appropriate correction(s) is (are) required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

5. Claims 1, 2, 4 – 6, 15 and 17 are rejected under 35 U.S.C. 102(e) as being anticipated by Burns (U.S. Patent 2004/0103317).

As per claim 1 and 5, Burns teaches a method in which a computer acquires particular data through a network, said method comprising steps of:

detecting an activation instruction to activate a particular program (Burns: Para [0026] Line 12 – 18 and Para [0016] Line 1 – 3: detecting a user remote log-in request application);

performing particular data acquisition processing for acquiring the particular data through the network, when an activation instruction to activate the particular program is

detected (Burns: Para [0017] Line 1 – 7 / Line 8 – 11 and Para [0015] Line 1 – 4: the security module acquires the security policy data to check whether the user computer is in compliance with the desired security policy); and

thereafter, activating said particular program whose activation has been instructed (Burns: Para [0017] Line 8 – 18: the user remote log-in request application is qualified as said particular program).

As per claim 15 and 17, Burns teaches a network security enhancing system for computer, wherein:

said network security enhancing system comprises a means that automatically generates a control program (Burns: Para [0016] Line 5 – 7, Para [0017] Line 1 – 7 / Line 8 – 11 and Para [0015] Line 1 – 4: the security module is qualified as the control program, which is not manually generated); and

said control program detects a program that is installed on the computer and connects to a network and sends and receives communications, activates processing of connecting to the network and processing of updating a security file, and thereafter activates said program that sends and receives communications (Burns: Para [0026] Line 12 – 18 and Para [0016] Line 1 – 3, Para [0017] Line 1 – 7 / Line 8 – 18 and Para [0015] Line 1 – 4: see the same rationale of rejection as above in claim 1).

As per claim 2, 4 and 6, Burns teaches said activation instruction to activate the particular program is an activation instruction to activate a program that sends and

receives communication (Burns: Para [0026] Line 12 – 18 and Para [0016] Line 1 – 3: activation of a user remote log-in request application, which is a program that sends and receives communication from the remote server).

6. Claims 1 – 17 are rejected under 35 U.S.C. 102(e) as being anticipated by Albert et al. (U.S. Patent 2003/0177389) – This also includes the reference incorporated by reference Freund et al. (U.S. Patent 2003/0055962) – see (Albert: Para [0096]).

As per claim 1 and 5, Albert teaches a method in which a computer acquires particular data through a network, said method comprising steps of:

detecting an activation instruction to activate a particular program (Albert: Para [0025], Para [0062] / [068] & Freund: Para [049], Para [0116], Para [0149] Line 13 – 17);

performing particular data acquisition processing for acquiring the particular data through the network, when an activation instruction to activate the particular program is detected (Albert: Para [0025], Para [0062] / [068] & Freund: Para [049], Para [0116], Para [0149] Line 13 – 17 and Figure 7 / Element 702: (a) the current security policy is generated / updated by merging a plurality of security policies (or updating a current virus software) related for governing a connection to a particular network and (b) only after the updated security policy is applied to the device, the connection from the device to that particular network is then allowed to proceed); and

thereafter, activating said particular program whose activation has been instructed (see the same rationale of rejection as above).

As per claim 7 and 16, Albert teaches a network security enhancing system for a computer, comprising:

a means that activates processing of updating a security file at activation of a program that connects to a network and sends and receives communications, after processing of connection to said network and before other processing (Albert: Para [0025], Para [0062] / [068] & Freund: Para [049], Para [0116], Para [0149] Line 13 – 17 and Figure 7 / Element 702: (a) the current security policy is generated / updated by merging a plurality of security policies (or updating a current virus software) related for governing a connection to a particular network and (b) only after the updated security policy is applied to the device, the connection from the device to that particular network is then allowed to proceed).

As per claim 15 and 17, Albert teaches a network security enhancing system for computer, wherein:

said network security enhancing system comprises a means that automatically generates a control program (Albert: Para [0024] Line 11 – 13: a security enforcement module); and

said control program detects a program that is installed on the computer and connects to a network and sends and receives communications, activates processing of connecting to the network and processing of updating a security file, and thereafter activates said program that sends and receives communications (Albert: Para [0025],

Para [0062] / [068] & Freund: Para [049], Para [0116], Para [0149] Line 13 – 17 and Figure 7 / Element 702: (a) the current security policy is generated / updated by merging a plurality of security policies (or updating a current virus software) related for governing a connection to a particular network and (b) only after the updated security policy is applied to the device, the connection from the device to that particular network is then allowed to proceed).

As per claim 2, 4 and 6, Albert teaches said activation instruction to activate the particular program is an activation instruction to activate a program that sends and receives communication (Albert: Para [0025], Para [0062] / [068] & Freund: Para [049], Para [0116], Para [0149] Line 13 – 17 and Figure 7 / Element 702: a program that governs a connection to a particular network is qualified as a particular program).

As per claim 3, Albert teaches said particular data acquisition processing is processing of updating a security file (Albert: Para [0025] and Para [0062]: (a) the current security policy is generated / updated by merging a plurality of security policies related for governing a connection to a particular network and (b) only after the updated security policy is applied to the device, the connection from the device to that particular network is then allowed to proceed).

As per claim 8, Albert teaches a means that displays a message reporting completion of said processing of updating the security file, after the processing has

been completed (Albert: Para [0062] / [0043]: capable to display the result of the operation which includes security policy update).

As per claim 9, Albert teaches a means that detects first activation of a program that connects to the network and sends and receives communications, in a state that an already-operating computer is not connected to the network; and a means that activates the processing of updating the security file at activation of said program, after processing of connection to said network and before other processing (Albert: Para [0025] and Para [0062] / [068]: security policy enforcement must be checked before any VPN connection can be proceeded).

As per claim 10, Albert teaches said processing of updating the security file is processing of acquiring amendment of a definition file used for an antivirus countermeasure (Freund: Para [049], Para [0116], Para [0149] Line 13 – 17 and Figure 7 / Element 702: displaying "the system has detected that you must update your current virus software" – which surely includes the current virus definition file).

As per claim 11, Albert teaches said processing of updating the security file is processing of acquiring a patch file (Freund: Para [0149] and Para [0149] Line 13 – 17: a security patch file applied to a non-compliant computer in order to continue t proceed a particular network connection).

As per claim 12, Albert teaches a means that activates the processing of updating the security file at activating a browser and before displaying a screen (Albert: Para [0025] & Freund: Para [0007], Para [0027] Para [0117] and Para [0149] Line 13 – 17: (a) updating a security policy on the connection to a particular network by (b) using WWW (i.e. web browser) for the connection to a large network (c) updating the security file at activating a browser for connecting to a particular large network and (d) the first screen will not be proceeded for security policy in-compliance – i.e. the remote log-on screen will not be displayed).

As per claim 13, Albert teaches a means that outputs a message requesting activation of the processing of updating the security file, after said program that connects to the network and sends and receives communications connects to the network and before said program starts communication operation (Freund: Para [049], Para [0116], Para [0149] Line 13 – 17 and Figure 7 / Element 702: displaying "the system has detected that you must update your current virus software" – which surely includes the current virus definition file) & (Albert: Para [0025] and Para [0062] / [068]: (a) the current security policy is generated / updated by merging a plurality of security policies related for governing a connection to a particular network and (b) only after the updated security policy is applied to the device, the connection from the device to that particular network is then allowed to proceed).

As per claim 14, Albert teaches a means that outputs a message requesting activation of the processing of updating the security file, at activation of a browser and before displaying a screen (Albert: Para [0025] & Freund: Figure 7 / Element 702 & Para [049], Para [0116], Para [0007], Para [0027] Para [0117] and Para [0149] Line 13 – 17: (a) displaying "the system has detected that you must update your current virus software" – which surely includes the current virus definition file (b) updating a security policy on the connection to a particular network by (c) using WWW (i.e. web browser) for the connection to a large network (d) updating the security file at activating a browser for connecting to a particular large network and (e) the first screen will not be proceeded for security policy in-compliance – i.e. the remote log-on screen will not be displayed).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Longbit Chai Ph.D.
Primary Patent Examiner
Art Unit 2431
7/29/2008